What is claimed is:

1. An encryption method for use by an encryption apparatus that encrypts plaintext data composed of a plurality of blocks, the encryption method comprising:

a block obtaining step for obtaining the plaintext data one block at a time in order from outside the encryption apparatus;

a selecting step for selecting either a first mode or a second mode for a current block obtained in the block obtaining step according to how many blocks have been obtained;

a key generating step for generating

(1) a first group composed of a predetermined number *n* of different subkeys when the first mode is selected, and

(2) a second group composed of less than *n* different subkeys when the second mode is selected; and

an encrypting step for encrypting the current block by subjecting the current block to *n* conversion processes in order, wherein

in the first mode, each of the *n* conversion processes is associated with a different subkey in the first group and is performed using the associated subkey, and

in the second mode, the *n* conversion processes are associated with subkeys in the second group and are each performed using the associated subkey.

2. An encryption method according to Claim 1,

wherein the selecting step selects

(i) the first mode for blocks whenever a number of blocks that have been obtained is equal to a multiple of a predetermined value, and

(ii) the second mode for all other cases.

3. An encryption method according to Claim 1,

wherein the encryption apparatus includes an initial value storing means for storing an initial value,

the encrypting step encrypts the current block to generate a ciphertext block having a predetermined length, and

the key generating step generates the first group using the initial value in the first mode and generates the second group using the initial value and the ciphertext block most recently generated by the encrypting step in the second mode.

4. An encryption apparatus for encrypting plaintext data composed of a plurality of blocks, the encryption apparatus comprising:

block obtaining means for obtaining the plaintext data one block at a time in order from outside;

selecting means for selecting either a first mode or a second mode for use with a current block obtained in the block obtaining means according to how many blocks have been obtained;

key generating means for generating

(1) a first group composed of a predetermined number *n* of different subkeys when the first mode is selected, and

(2) a second group composed of less than *n* different subkeys when the second mode is selected; and

encrypting means for encrypting the current block by subjecting the current block to *n* conversion processes in order, wherein

in the first mode, each of the *n* conversion processes is associated with a different subkey in the first group and is performed using the associated subkey, and

in the second mode, the *n* conversion processes are each associated with a subkey in the second group and are each performed using the associated subkey.

5. A computer-readable storage medium storing an encryption program for use by a computer that encrypts plaintext data composed of a plurality of blocks,

the encryption program comprising:

a block obtaining step for obtaining the plaintext data one block at a time in order from outside the encryption apparatus;

a selecting step for selecting either a first mode or a second mode for a current block obtained in the block obtaining step according to how many blocks have been obtained;

a key generating step for generating

(1) a first group composed of a predetermined number *n* of different subkeys when the first mode is selected, and

(2) a second group composed of less than *n* different subkeys when the second mode is selected; and

an encrypting step for encrypting the current block by subjecting the current block to *n* conversion processes in order, wherein

in the first mode, each of the *n* conversion processes is associated with a different subkey in the first group and is performed using the associated subkey, and

in the second mode, the *n* conversion processes are associated with subkeys in the second group and are each performed using the associated subkey.

6. A decryption method for use by a decryption apparatus that decrypts ciphertext data in ciphertext block units, the decryption method comprising:

a block obtaining step for obtaining the ciphertext data one ciphertext block at a time in order from outside the decryption apparatus;

a selecting step for selecting either a first mode or a second mode for use with a current ciphertext block obtained in the block obtaining step according to how many ciphertext blocks have been obtained;

a key generating step for generating

(1) a first group composed of a predetermined number *n* of different subkeys when the first mode is selected and

(2) a second group composed of less than *n* different subkeys when the second mode is selected; and

a decrypting step for decrypting the current ciphertext block by subjecting the current ciphertext block to *n* conversion processes in order, wherein

in the first mode, each of the *n* conversion processes is associated with a different subkey in the first group and is performed using the associated subkey, and

in the second mode, the *n* conversion processes are associated with subkeys in the second group and are each performed using the associated subkey.

7. A decryption method according to Claim 6,

wherein the selecting step selects

(1) the first mode whenever a number of ciphertext blocks that have been obtained is given as a multiple of a predetermined value, and

(2) the second mode for all other cases.

8. A decryption method according to Claim 6,

wherein the decryption apparatus includes an initial value storing means for storing an initial value,

the key generating step generating the first group using the initial value in the first mode and generating the second group using the initial value and the ciphertext block obtained immediately before the current ciphertext block in the second mode.

9. A decryption apparatus that decrypts ciphertext data in ciphertext block units, the decryption apparatus comprising:

block obtaining means for obtaining the ciphertext data one ciphertext block at a time in order from outside;

selecting means for selecting either a first mode or a second mode for use with a current ciphertext block obtained by the block obtaining means according to how many ciphertext blocks have been obtained;

key generating means for generating

(1) a first group composed of a predetermined number *n* of different subkeys when the first mode is selected, and

(2) a second group composed of less than *n* different subkeys when the second mode is selected; and

decrypting means for decrypting the current ciphertext block by subjecting the current ciphertext block to *n* conversion processes in order, wherein

in the first mode, each of the *n* conversion processes is associated with a different subkey in the first group and is performed using the associated subkey, and

in the second mode, the *n* conversion processes are associated with subkeys in the second group and are each performed using the associated subkey.

10. A computer-readable storage medium storing a decryption program for use by a computer that decrypts ciphertext data in ciphertext block units,

the decryption program comprising:

a block obtaining step for obtaining the ciphertext data one ciphertext block at a time in order from outside the decryption apparatus;

a selecting step for selecting either a first mode or a second mode for use with a current ciphertext block obtained in the block obtaining step according to how many ciphertext blocks have been obtained;

a key generating step for generating

(1) a first group composed of a predetermined number *n* of different subkeys when the first mode is selected and

(2) a second group composed of less than *n* different subkeys when the second mode is selected; and

a decrypting step for decrypting the current ciphertext block by subjecting the current ciphertext block to *n* conversion processes in order, wherein

in the first mode, each of the *n* conversion processes is associated with a different subkey in the first group and is performed using the associated subkey, and

in the second mode, the *n* conversion processes are associated with subkeys in the second group and are each performed using the associated subkey.